CRIMSON PUBLISHERS
Wings to the Research

Research in
Medical & Engineering Sciences

ISSN: 2576-8816

Mini Review

A Proposed Method for Image Steganography

Samir Kumar Bandyopadhyay*

Advisor to Chancellor, India

***Corresponding author:** Samir Kumar Bandyopadhyay, Advisor to Chancellor, India

Submission: December 11, 2017; **Published:** February 15, 2018

Abstract

All security techniques try to maintain Confidentiality, Integrity and Availability- referred to as the CIA Triad of information security. Steganography also takes a real challenge in the field of security through data concealment. A Steganography System consists of two functions: embedding and extraction. The objective of the proposed work is to design robust algorithms which generate stego media, can carry large amount (capacity) of secret data without reducing imperceptibility.

Introduction

Today internet has become a trusted factotum of everyone. Almost all payments like tax, insurance, bank transaction, healthcare payment, payment in e-commerce are done digitally through debit or credit card or through e-wallet. People share their personal information through social media like Facebook. Twitter, Whatsapp etc. The government of every developing country is going to embrace e-Governance system to interact with people more promptly. The information shares through these applications are the burning target to intruders [1]. Different techniques are already plays an important role in the field to information security for a long decade. The famous one is cryptography that keeps the content of the message secret, but it is not sufficient at all. On the other hand the watermarking hides data to keep copyright related information [2]. It is also not secure at all because many techniques are available to remove watermark easily. Now-a-days people prefer a system that hides the existence of message secret. The technique, Steganography highlights the concept of security through obscurity.

The word "Steganography" is the combination of two Greek words Stegano (Cover) and Grafia (Writing) and its aim is "to hide in plain sight" [3]. It has been used throughout 2500 years and was coined at the end of the 15th Century after the appearance of Trithemius book on the subject "Steganographia". Modern steganography is generally understood to deal with electronic media rather than physical objects. The synopsis introduces noble methods of steganography by considering Image and Audio as cover media.

The rapid use of digital images for communication through internet makes image a popular cover media in steganography. Not only this reason, there are some other factors like content adaptability, redundancy, limited power of HVS, continuous growth of strong graphics power in computer, and the fruitful contribution of the researcher in the field of digital image processing also stand behind this popularity [4]. The reason for considering audio as cover media is the representation of amplitudes in real number format causes very small distortions after embedding the bits of target data. Instead of that the audio also has some unique characteristics like gradual change in amplitudes rather than sudden change, high frequency suppress lower frequency components etc., whereas the strong sensitivity of Human Auditory System (HAS) makes audio steganography a more challenging security technique [5].Literature Survey

The better understanding on different state-of-the-art works is very helpful for the validation of new implementation and also analyzing its performance accuracy in terms of security. The synopsis starts with the solution of the loopholes of standard LSB technique and then tries to enrich the thoughts. The standard LSB technique is very easy to implement where the Least Significant bit of a pixel/samples of cover media is replaced with target bit [6]. The method can preserve imperceptibility but suffers from low robustness and capacity. T. Penvy et al. introduce a secure steganography algorithm HUGO which can able to defeat almost all steganalysis attacks by defining distortion based on feature vector already used in steganalysis. It supports capacity of stego media seven times more than standard LSB technique. However, the results were not satisfying at all in the case of multi-bit approach BC Nguyen et al. [7] improves the capacity of LSB substitution techniques by introducing popular multi bit-plane image steganography technique. The increase in capacity again reduces imperceptibility WC Kuo et al. [8]. increases capacity by embedding multiple bits of target data encoded through run-length encoding (RLE), but maintain imperceptibility by considering Multi-bit Generalized Exploiting Modification Direction (MGEMD) characteristics. MGEMD features not only reduce distortion but

help to resist modern steganalysis attacks [9]. The all above discussed does not meet robustness up to the level. The robustness of the LSB Substitution technique may increase by embedding data at higher LSB layer or through embedding at random positions of the cover and also introducing double layer security N Cvejic et al. [10]. In their work embeds target data at the higher bit-plane then preserves quality through bit adjustment. The method also spread out the embedding error to the four predecessors' samples of the current sample. Although embedding at higher bit-plane increase robustness but the involvement of five samples for hiding of single bits of target data loses capacity [10]. K Gopalan in [11] provides double layer security by embedding encrypted data bits into the k-th layer of Audio samples. The method increases robustness as well as imperceptibility by using the nature of human auditory system. The low robustness problem due to embedding at higher bit-plane is solved by decomposition the intensity into another number system which uses more bits to represent the number in the range 0 to 255. F. Battisti et al first introduce this concept in steganography based on Zeckendorf's theorem. They use general Fibonacci sequence for generating virtual bit-planes and then perform embedding in those bit-planes [12,13]. The robustness and the imperceptibility of proposed method is enhanced through value adjustment rather direct replacement of cover bits with target data. In [14] the secret message is embedded within the host image without hampering imperceptibility based on a smart pixel adjustment policy with two averages of the block. The resultant stego images can tolerate the manipulations such as edge sharpening, inversion, color quantization, pixel-truncation, JPEG, and etc. In [15] MOD-4 technique is used for embedding two bits of target data in each R, G and B plane of cover pixel thus 6 bits in each pixel, helps in enhance capacity. The method just embeds two target bits and do not consider the boundary value problem.

The major problem in steganography is the negative effect on the visual quality. Region based steganography solves this problem by embedding data at certain region selected based on the characteristics of HVS and image attributes. Most of the binary image Steganographic techniques consider the flipping distortion according to HVS although these are not secure to steganalysis attacks. Feng et al. in [16] solves this issue by measuring the distortion based on the complement, rotation, and mirroring-invariant local texture patterns (crmiLTPs) and use syndrome-trellis code (STC) for minimizing distortion. K Qazanfari et al. [17]. Maintain the statistical and perceptual attributes of the cover image in the stego media by completely preserving the cover histogram. Their LSB++ method causes lower distortion in the co-occurrence matrices by protecting the sensitive pixels from extra bit embedding. Their method is more capacitive and maintains histogram of JPEG images.

Proposed Work

The proposed work is to design robust algorithms for doing the followings:

A. Improve robustness through random and virtual bit-plane embedding rather than static layer embedding, through value amendment technique instead direct replacement of bits, through embedding at selected region than consecutive pixels/samples.

B. Preserve Imperceptibility through bit adjustment or value adjustment and by considering the characteristics of human perception.

C. Increase Capacity through multi-bit embedding in 24 bit image as well as audio and through compressed data embedding.

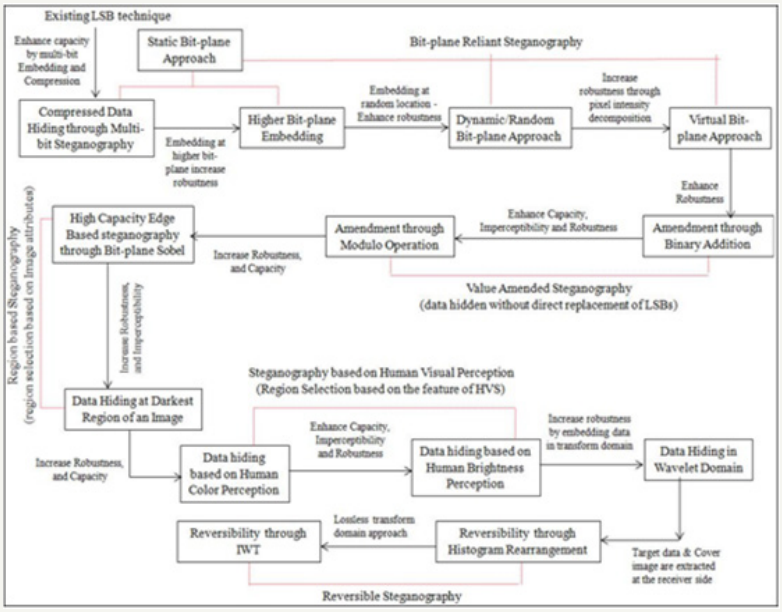

Figure 1: Block Diagram of the Proposed Method.

How to cite this article: Samir K B. A Proposed Method for Image Steganography. Res Med Eng Sci. 3(4). RMES.000569.2018.
DOI: 10.31031/RMES.2018.03.000569

In a nutshell the whole work tries to reduce the rate of inverse proportion among the three challenges of steganography. The performance of the proposed method is evaluated based on different Image Quality Assessment Metrics (IQAMs) (e.g. PSNR, NCC, LMSE, SSIM etc.), Bit-plane analysis, statistical test (histogram differences, Chi-square attack), structural attacks (SP, WS etc.), different steganalysis attacks like RS attack etc. A standard benchmark tool-Stir Mark Benchmark is used for analyzing the performance of proposed method based on different parameters. The security strength of the algorithms is measured through KL divergence and the capacity of the stego image based on bpp. The following Figure 1 shows the flow of the proposed method.

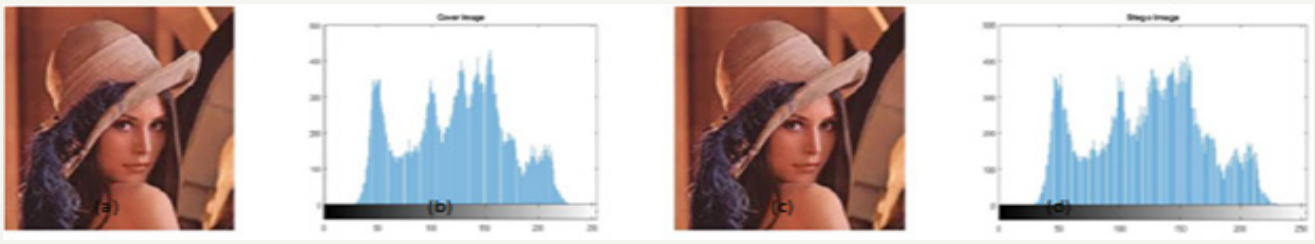

Figure 2: (a) Cover Image (b) Cover Histogram (c) Stego Image (d) Stego Histogram and PSNR is 45.16.

The sample results are shown in Figure 2. The method enhances the capacity by embedding a character within a pixel using 2-2-2 format instead 3-3-2 (which is used in most of the cases for 8 bit ASCII) which again helps to preserve quality of stego media. But the method does not show any attractive solution for the improvement of robustness.

Conclusion

The method begins with the solution of low capacity issue in standard LSB technique by hiding multiple bits in a pixels/samples. The problem of low robustness is solved by embedding data at the higher LSB layer of both image and audio. The techniques become more robust by considering multiple bit-planes randomly for embedding target data and also perform embedding in virtual bit-planes. The imperceptibility as well as the robustness of steganography techniques are increased by embedding multiple bits in a particular region selected either based on some image attributes or by Human Visual Perception. The synopsis is also highlights the advantages of transform domain techniques over spatial domain and embed data in DWT domain. On the other hand the research on reversible steganography helps in effective application of the proposed research works in real scenario. All of the techniques are analyzed based on different assessment metrics. The resistance is tested against different steganalysis attacks. The analysis helps to prove correctness, whereas the comparison with the state-of-the-art-works helps in validation of this research in the field of security.

References

1. Shu X, Zhang J, Yao DD, Feng WC (2016) Fast detection of transformed data leaks. IEEE Transactions on Information Forensics and Security 11(3): 528-542.
2. Bergman M (2016) It's hard to get good (security) help these days. IEEE Consumer Electronics Magazine 5(3): 132-133.
3. Jamil T (1999) Steganography: The art of hiding information is plain sight. IEEE Potentials 18(1): 10-12.
4. Martin A, Sapiro G, Seroussi G (2005) Is image steganography natural? IEEE Trans Image Process 14(12): 2040- 2050.
5. Kekre HB, Athawale A, Rao S, Athawale U (2010) Information hiding in audio signals. International Journal of Computer Applications 7(9): 14-19.
6. Basu PN, Bhowmik T (2010) On embedding of text in audio - a case of steganography. in proc of IEEE International Conference on Recent Trends in Information, Telecommunication and Computing, India.
7. Pevny T, Filler T, Bas P (2010) Using high-dimensional image models to perform highly undetectable steganography. Information Hiding 6387: 161-177.
8. Nguyen BC, Yoon SM, Lee HK (2006) Multi bit plane image steganography. International Workshop on Digital Watermarking 4283: 61-70.
9. Kuo WC, Kuo SH, Wu LC (2015) Multi-bit data hiding scheme for compressing secret messages. Appl Sci 5(4): 1033-1049.
10. Cvejic N, Seppanen T (2005) Reduced distortion bit-modification for LSB audio steganography. Journal of Universal Computer Science 11(1): 56-65.
11. Gopalan K, Shi Q, (2010) Audio steganography using bit modification - a tradeoff on perceptibility and data robustness for large payload audio embedding. in Proc of IEEE 19th International Conference on Computer Communications and Networks (ICCCN), Switzerland.
12. Mammia E, Battisti F, Carlia M, Neria A, Egiazarianb K, et al. (2008) A novel spatial data lhiding scheme based on generalized Fibonacci sequences. in Proc of SPIE, Mobile Multimedia/Image Processing, Security, and Applications 6982: 1-7.
13. Pund-Dange S, Desai CG (2017) Data hiding technique using catalan-lucas number sequence. Indian Journal of Science and Technology 10(4): 1-6.
14. Yang CY, Wang WF (2015) Block-based colour image steganography using smart pixel-adjustment. Genetic and Evolutionary Computing 329: 145-154.
15. Chugh G, Yadav R, Saini R (2014) A new image steganographic approach based on mod factor for RGB images. International Journal of Signal Processing, Image Processing and Pattern Recognition 7(3): 27-44.
16. Feng B, Lu W, Sun W (2015) Secure binary image steganography based on minimizing the distortion on the texture. IEEE Transactions on Information Forensics and Security 10(2): 243-255.
17. Qazanfari K, Safabakhsh R (2014) A new steganography method which preserves histogram: generalization of LSB++. Elsevier Journal of Information Sciences 277: 90-101.

For possible submission use the below is the URL **Submit Article**

How to cite this article: Samir K B. A Proposed Method for Image Steganography. Res Med Eng Sci. 3(4). RMES.000569.2018.
DOI: 10.31031/RMES.2018.03.000569